УДК 519.1

В. К. Медведев

Об одном подходе к построению конечных тернарных колец

Напомним некоторые факты из теории проективных плоскостей. Каждой проективной плоскости P можно сопоставить тернарное кольцо A [1], т. е. отображение $\Phi : A \times A \times A \to A$, удовлетворяющее следующим аксиомам (здесь Φ (abc) обозначается через $\langle abc \rangle$):

Т1. Уравнение $\langle abx \rangle = c$ имеет и единственное решение при любых элементах a, b, c из A;

Т2. Уравнение $\langle axb \rangle = \langle cxd \rangle$ имеет и единственное решение при любых элементах a, b, c, d из A таких, что $a \neq c$;

Т3. Система уравнений

$$\begin{cases} \langle xay \rangle = b, \\ \langle xcy \rangle = d \end{cases}$$

имеет единственное решение при любых элементах a, b, c, d из A таких, что $a \neq c$. Наоборот, всякому тернарному кольцу можно сопоставить проективную плоскость [1].

Отметим, что в случае конечного тернарного кольца A (когда множество A конечно) из аксиом Т1 и Т2 следует аксиома Т3. Это есть следствие того факта, что если в конечной системе инцидентности $S = (P, B, I)$ каждый элемент из P принадлежит одному и тому же числу k блоков из B, каждый блок $b \in B$ содержит одно и то же число k элементов из P и любые два различных блока содержат ровно λ общих элементов (для нас важен случай $\lambda = 1$), то любая пара различных элементов встречается ровно в λ различных блоках [1].

Пусть G (F) — проективная плоскость Галуа, где F — поле. В этом случае множество элементов поля F с операцией $\langle abc \rangle = ab + c$ есть соответствующее этой плоскости тернарное кольцо [1]. Введем на множестве F новую тернарную операцию $\langle abc \rangle_{\varphi,\psi} = ab + \psi(b)\, c + \varphi(a)$, где φ и ψ — функции из F в F (иными словами, новая тернарная операция есть некоторая «деформация» прежней с помощью функций φ и ψ). Найдем условия на функции φ и ψ, при которых операция $\langle abc\rangle_{\varphi,\psi}$ есть тернарное кольцо. Приведем основной результат статьи.

Теорема 1. *Пусть поле F конечно. Тернарная операция $\langle abc\rangle_{\varphi,\psi}$ есть тернарное кольцо тогда и только тогда, когда для любого элемента $a \in F$ $\psi(a) \neq 0$ и для множества A_φ всех элементов поля F вида $\frac{\varphi(a_1)-\varphi(a_2)}{a_1-a_2}$, где $a_1 \in F$, $a_2 \in F$, $a_1 \neq a_2$ и множества B_ψ всех элементов из $F \cup \infty$ вида*

$$\frac{\psi(b_1)\,b_2-\psi(b_2)\,b_1}{\psi(b_2)-\psi(b_1)},$$

где $b_1 \in F$, $b_2 \in F$, $b_1 \neq b_2$ имеет место соотношение $A_\varphi \cap B_\psi = \varnothing$.

Доказательство. Условие $\psi(a) \neq 0$ при любом элементе $a \in F$, очевидно, необходимо и достаточно для того, чтобы тернарная операция $\langle\ \ \rangle_{\varphi,\psi}$ удовлетворяла аксиоме T1. Выполнение аксиомы T2 для операции $\langle\varphi, \psi\rangle$ равносильно тому, что уравнение

$$(a-c)\,x+\varphi(a)-\varphi(c)=\psi(x)(b-d) \tag{1}$$

имеет единственное решение относительно $x \in F$ при любых элементах a, b, c, d из F таких, что $a \neq c$. Если $b = d$, то этот факт имеет место в любом случае. Поэтому рассмотрим случай, когда $b \neq d$. Уравнение (1) при этом равносильно уравнению

$$\frac{a-c}{e}\,x+\frac{\varphi(a)-\varphi(c)}{e}=\psi(x), \tag{2}$$

где $e = b-d$, $e \neq 0$. Таким образом, выполнение аксиомы T2 для операции $\langle\ \ \rangle_{\varphi,\psi}$ равносильно тому, что уравнение (2) имеет единственное решение относительно $x \in F$ при любых элементах a, c, e из F таких, что $a \neq c$, $e \neq 0$. Иными словами, любая прямая вида $y=\frac{a-c}{e}x+\frac{\varphi(a)-\varphi(c)}{e}$, где $a \neq c$, $e \neq 0$, должна пересекать график функции $y=\psi(x)$ и только в одной точке. Рассмотрим семейство U всех прямых на плоскости вида

$$y=\frac{a-c}{e}\,x+\frac{\varphi(a)-\varphi(c)}{e},$$

где $a \neq c$, $e \neq 0$. Это есть в точности семейство всех прямых, не параллельных прямой $x = 0$, отличных от прямой $y = 0$ и пересекающих прямую $y = 0$ в точках множества V, где V есть множество всех точек на прямой $y = 0$, для координаты x которых выполнено условие $-x \in A_\varphi$. Любая прямая, пересекающая график функции $\psi(x)$ по крайней мере в двух точках $(x_1, \psi(x_1))$, $(x_2, \psi(x_2))$, $x_1 \neq x_2$, не параллельна оси $x = 0$ и пересекает прямую $y = 0$ только при $\varphi(x_1) \neq \varphi(x_2)$ в точке с координатой

$$x=-\frac{\psi(x_1)\,x_2-x_1\psi(x_2)}{\psi(x_2)-\psi(x_1)}$$

и, таким образом, $-x \in B_\psi$. В частности, через любую точку на прямой $y = 0$, для координаты x_0 которой выполнено условие $-x_0 \in B_\psi$, можно провести прямую, не параллельную прямой $x = 0$ и пересекающую график функции ψ в двух точках. Таким образом, условие $A_\varphi \cap B_\psi = \varnothing$ является необходимым условием для того, чтобы выполнялась аксиома T2. Покажем, что оно является и достаточным для выполнения аксиомы T2.

Действительно, пусть $A_\varphi \cap B_\psi = \varnothing$. Любая прямая, не параллельная прямой $x = 0$, отличная от прямой $y = 0$ и проходящая через любую точку множества V, принадлежит семейству U. Для каждой точки $a \in V$ число таких прямых, проходящих через точку a, равно $|F|-1$. Соединим точку a прямой с любой точкой $(u, \psi(u))$ на графике функции ψ, где u не равно координате x точки a. Тогда эта прямая не параллельна прямой $x = 0$, отлична от прямой $y = 0$ (поскольку $\psi(u) \neq 0$ при любом u). Следовательно, она принадлежит семейству U и, таким образом, пересекает график функции ψ только в точке $(u, \psi(u))$ (в силу условия $A_\varphi \cap B_\psi = \varnothing$). Число точек $(u, \psi(u))$ на графике функции ψ, для которых u не равно координате x точки a, равно $|F| - 1$. Таким образом, каждая прямая из семейства U, проходящая через любую точку $a \in V$ (т. е. каждая прямая семейства U), пересекает график функции ψ и только в одной точке. Следовательно, уравнение (2) имеет и единственное решение при любых $a \neq c$, $e \neq 0$ и теорема доказана.

Пусть $\psi(a) \neq 0$ при любом элементе $a \in F$. Множество B_ψ всех элементов из $F \cup \infty$ вида $\frac{\psi(x) y - x\psi(y)}{\psi(y) - \psi(x)}$, где $x \neq y$ совпадает с множеством всех элементов из $F \cup \infty$ вида $-\frac{xu(x) - yu(y)}{u(x) - u(y)}$, где $x \neq y$, а $u(x) = \frac{1}{\psi(x)}$ (это непосредственно видно, если разделить и числитель и знаменатель выражения $\frac{\psi(x) y - x\psi(y)}{\psi(y) - \psi(x)}$ на $\psi(x)\psi(y)$). Для любой функции $u: F \to F$, где $u(a) \neq 0$ при любом элементе $a \in F$, множество всех элементов из $F \cup \infty$ вида $-\frac{u(x)x - u(y)y}{u(x) - u(y)}$ обозначим через B'_u, так что $B'_u = B_{u^{-1}}$.

Предложение 1. *Пусть F — конечное поле. Каждая пара функций u и φ из F в F такая, что $A_\varphi \cap B'_u = \varnothing$ и $u(a) \neq 0$ при любом элементе $a \in F$, определяет тернарное кольцо.*

Доказательство. Рассмотрим тернарное кольцо $\langle\ \rangle_{\varphi, u^{-1}}$. Теперь предложение есть следствие теоремы 1.

Для любых двух функций τ_1, τ_2 из F в F таких, что $\tau_2(a) \neq 0$ при любом элементе $a \in F$ и отображение $x \to \frac{\tau_1(x)}{\tau_2(x)}$ есть взаимно-однозначное отображение поля F на себя, определим подмножество $B_{\tau_1, \tau_2} \subset F \cup \infty$ множества $F \cup \infty$, как совокупность всех элементов из $F \cup \infty$ вида $-\frac{\tau_1(x) - \tau_1(y)}{\tau_2(x) - \tau_2(y)}$, при $x \neq y$, $x \in F$, $y \in F$. Отметим, что при $x \neq y$ не может быть равенств $\tau_1(x) - \tau_1(y) = 0$, $\tau_2(x) - \tau_2(y) = 0$ одновременно, так что выражение $\frac{\tau_1(x) - \tau_1(y)}{\tau_2(x) - \tau_2(y)}$ определено как элемент из $F \cup \infty$.

Лемма 1. *Пусть функции τ_1, τ_2 из F в F таковы, что $\tau_2(a) \neq 0$ при любом элементе $a \in F$ и отображение $x \to \frac{\tau_1(x)}{\tau_2(x)}$ есть взаимно-однозначное отображение поля F на себя. Тогда $B_{\tau, \tau_2} = B'_u$ для некоторой функции u из F в F такой, что $\tau_2(a) \neq 0$ при любом элементе $a \in F$. Наоборот, для любой функции u из F в F существуют функции τ_1, τ_2 из F в F такие, что $\tau_2(a) \neq 0$ при любом элементе $a \in F$, отображение $x \to \frac{\tau_1(x)}{\tau_2(x)}$ есть взаимно-однозначное отображение из F в F и $B'_u = B_{\tau_1, \tau_2}$.*

Доказательство. Пусть для функций τ_1, τ_2 из F в F, $\tau_2(a) \neq 0$ при любом элементе $a \in F$ и отображение $x \to \frac{\tau_1(x)}{\tau_2(x)}$ из F в F взаимно-однозначно. Сделаем замену переменных $\frac{\tau_1(x)}{\tau_2(x)} = z$. Тогда $\tau_2(x) = u(z)$ для некоторой функции u из F в F, $\tau_1(x) = zu(z)$ и выражение $-\frac{\tau_1(x) - \tau_1(y)}{\tau_2(x) - \tau_2(y)}$ приобретает вид $-\frac{z_1 u(z_1) - z_2 u(z_2)}{u(z_1) - u(z_2)}$. Таким образом, $B_{\tau_1, \tau} = B'_u$ и, кроме того, $u(a) \neq 0$ при любом элементе $a \in F$. Наоборот пусть u отображение из F в F, $u(a) \neq 0$ при любом элементе $a \in F$. Положим $\tau_2(x) = u(x)$, $\tau_1(x) = xu(x)$. Тогда $B'_u = B_{\tau_1, \tau_2}$, $\tau_2(a) \neq 0$ при любом элементе $a \in F$ и отображение $x \to \frac{\tau_1(x)}{\tau_2(x)}$ из F в F взаимно-однозначно.

Из леммы 1 и предложения 1 непосредственно следует следующее предложение.

Предложение 2. *Пусть F — конечное поле. Каждой тройке функций φ, τ_1, τ_2 из F в F такой, что:*

1) *$\tau_2(a) \neq 0$ при любом элементе $a \in F$ и отображение $x \to \frac{\tau_1(x)}{\tau_2(x)}$ есть взаимно-однозначное отображение из F в F;*

2) *$A_\varphi \cap B_{\tau_1,\tau_2} = \varnothing$, где A_φ есть множество всех элементов поля F вида $\frac{\varphi(x)-\varphi(y)}{x-y}$ при $x \neq y$, а B_{τ_1,τ_2} есть множество всех элементов из $F \cup \infty$ вида $-\frac{\tau_1(x)-\tau_1(y)}{\tau_2(x)-\tau_2(y)}$, $x \neq y$, соответствует тернарное кольцо.*

Отметим, что теорема 1, предложения 1 и 2 равносильны.

Приведем один подход к построению функций φ и ψ, удовлетворяющих условиям теоремы 1.

Лемма 2. *Пусть F — поле, U — подгруппа мультипликативной группы F^* поля F, $\{c_i\}_{i\in I}$ — некоторый фиксированный полный набор представителей классов смежности группы F^* по подгруппе U. Пусть для любого элемента $x \in F^*$, $\tau_2(x) = c_i$, где c_i — данный представитель класса смежности xU, $\tau_1(x) = c_i x^{-1} \in U$. Пусть $\tau_1(0) = 0$, $\tau_2(0) = a_0$, где a_0 — произвольный элемент поля F, $a_0 \neq 0$. Тогда $\tau_2(a) \neq 0$ при любом элементе $a \in F$ и отображение $x \to \frac{\tau_1(x)}{\tau_2(x)}$ из F в F взаимно-однозначно.*

Доказательство очевидно.

Предложение 3. *Пусть F — конечное поле порядка q^2. Пусть Z_{q+1} — группа всех корней степени $q+1$ из 1 поля F (очевидно, что $|Z_{q+1}| = q+1$, $Z_{q+1} \subset F^*$). Тогда всякий полный набор $\{c_i\}_{i=1,\ldots,q-1}$ представителей классов смежности группы F^* по группе Z_{q+1} такой, что при любых $i \neq j$ уравнение $x^2-(c_i-c_j)x+(c_i-c_j)^{1-q}=0$ не имеет решения в поле F, являющегося корнем степени $q+1$ из 1, определяет тернарное кольцо на множестве F.*

Доказательство. Пусть $\varphi(x) = x^q$, функции τ_1 и τ_2 из F в F выбраны в соответствии с леммой 2 для $U = Z_{q+1}$ (и некоторого произвольного элемента $a_0 \in F$, $a_0 \neq 0$). Группа Z_{q+1} есть группа всех элементов поля F вида x^{q-1}, где $x \in F^*$. Это следует из того, что группа F^* циклическая порядка $(q+1)(q-1)$, а порядок ее подгруппы Z_{q+1} равен $q+1$. Отсюда $A_\varphi = Z_{q+1}$. Множество B_{τ_1,τ_2} есть, очевидно, объединение двух множеств $B^{(1)}_{\tau_1,\tau_2}$ и $B^{(2)}_{\tau_1,\tau_2}$, где $B^{(1)}_{\tau_1,\tau_2}$ есть совокупность всех элементов из $F \cup \infty$ вида $\frac{\xi_1-\xi_2}{c_i-c_j}$, при некоторых i, j, $\xi_1 \in Z_{q+1}$, $\xi_2 \in Z_{q+1}$, а $B^{(2)}_{\tau_1,\tau_2}$ есть совокупность всех элементов из $F \cup \infty$ вида $\frac{\xi}{a_0-c_i}$, где $\xi \in Z_{q+1}$, $i = 1, \ldots, q-1$ (при этом $B^{(1)}_{\tau_1,\tau_2}$ соответствует элементам из $F \cup \infty$ вида $\frac{\tau_1(x)-\tau_1(y)}{\tau_2(x)-\tau_2(y)}$ при $x \neq 0$, $y \neq 0$, а $B^{(2)}_{\tau_1,\tau_2}$ — элементам вида $\frac{\tau_1(x)-\tau_1(y)}{\tau_2(x)-\tau_2(y)}$, где либо $x = 0$, либо $y = 0$). При этом $B^{(1)}_{\tau_1,\tau_2} \cap A_\varphi = \varnothing$. Действительно, предположим, что это не так. Тогда $\frac{\xi_1-\xi_2}{c_i-c_j} = \xi_3$ для некоторых элементов ξ_1, ξ_2, ξ_3 из группы Z_{q+1} и некоторых i, j. Отсюда $\xi_1'-\xi_2' = c_i-c_j$, где $\xi_1' = \xi_1/\xi_3$, $\xi_2' = \xi_2/\xi_3$, $\xi_1' \in Z_{q+1}$, $\xi_2' \in Z_{q+1}$. Однако для произвольного поля L, $\operatorname{char} L = p > 0$ из уравнения $x-y = A$, где $A \in L$, можно определить x и y, если известно, что x и y есть корни степени p^k+1 из 1 для некоторого k.

Действительно, возводя обе части равенства $x-y = A$ в степень p^k, получаем $\frac{1}{x}-\frac{1}{y} = A^{p^k}$, откуда $xy = -A^{1-p^k}$, и как x, так и $-y$ являются корнями уравнения $x^2-Ax+A^{1-p^k} = 0$. Отсюда, как ξ_1', так и $-\xi_2'$, являются корнями уравнения $x^2-(c_i-c_j)x+(c_i-c_j)^{1-q} = 0$. Пришли к противоречию. Таким образом, $B^{(1)}_{\tau_1,\tau_2} \cap A_\varphi = \varnothing$. Покажем, что можно подобрать такой элемент $a_0 \in F$, $a_0 \neq 0$, что $B^{(2)}_{\tau_1,\tau_2} \cap A_\varphi = \varnothing$. Предположим, что это не так. Тогда для произвольного элемента $a_0 \in F^*$ найдется $i \in \{1, \dots, q-1\}$, что $\dfrac{-\xi_1}{a_0 - c_i} = \xi_2$ для некоторых элементов $\xi_1 \in Z_{q+1}$, $\xi_2 \in \in Z_{q+1}$, откуда $a_0 \in c_i + Z_{q+1}$. Следовательно, $F^* \subset \bigcup\limits_i (c_i + Z_{q+1})$. Но $\left|\bigcup\limits_i (c_i + Z_{q+1})\right| \leqslant \sum\limits_i |c_i + Z_{q+1}| = |F^*|$. Отсюда $F^* = \bigcup\limits_i (c_i + Z_{q+1})$. Но если c_{i_0} есть представитель класса смежности Z_{q+1}, то $0 \in c_{i_0} + Z_{q+1}$. Получаем противоречие. Таким образом, существует элемент $a_0 \in F^*$, что $B^{(2)}_{\tau_1,\tau_2} \cap A_\varphi = \varnothing$ (легко видеть, что такой элемент единствен). Теперь осталось применить предложение 2 к функциям φ, τ_1, τ_2. Предложение доказано.

В случае, когда $p \neq 2$, имеет место следующее следствие предложения 3.

Следствие 1. *Пусть для квадратичного расширения полей $F_q \subset \subset F_{q^2}$, $\operatorname{char} F_q \neq 2$ $\{c_i\}_{i=1,\dots,q-1}$ — полная система представителей классов смежности группы $F^*_{q^2}$ по группе корней $(q+1)$-й степени из 1. Пусть $\dfrac{1}{4} - N(c_i - c_j)^{-1}$ есть квадратичный вычет поля F_q при любых $i \neq j$. Тогда система представителей $\{c_i\}_{i=1,\dots,q-1}$ определяет конечную проективную плоскость порядка q^2.*

Примечание. $N(x)$ — норма расширения $F_q \subset F_{q^2}$, так что $N(x) = = x^{q+1}$.

Доказательство. Пусть при некоторых $i \neq j$ квадратное уравнение $x^2 - (c_i - c_j)x + (c_i - c_j)^{1-q} = 0$ имеет решение в группе корней Z_{q+1} $(q+1)$-й степени из 1. Тогда для некоторого $\xi \in Z_{q+1}$ $\xi + + \dfrac{(c_i - c_j)^{1-q}}{\xi} = c_i - c_j$ или $\dfrac{\xi}{c_i - c_j} + \dfrac{1}{(c_i - c_j)^q \xi} = 1$.

Последнее равенство равносильно тому, что $\operatorname{tr}\left(\dfrac{\xi}{c_i - c_j}\right) = 1$, где tr — след расширения $F_q \subset F_{q^2}$. Поскольку каждый элемент поля F_{q^2} имеет вид $x + y\sqrt{d}$, где x, y, d — элементы поля E_q, d — квадратичный невычет поля F_q, то $\dfrac{\xi}{c_i - c_j} = \dfrac{1}{2} + y\sqrt{d}$ для некоторого $y \in F_q$ (отметим, что $\operatorname{tr}(x + y\sqrt{d}) = 2x$, $N(x + y\sqrt{d}) = x^2 - dy^2$). Отсюда $N\left(\dfrac{\xi}{c_i - c_j}\right) = \dfrac{1}{4} - - dy^2$ или $N(c_i - c_j)^{-1} = \dfrac{1}{4} - dy^2$. Таким образом, $\dfrac{1}{4} - N(c_i - c_j)^{-1}$ есть квадратичный невычет поля F_q, что противоречит условию. Следовательно, уравнение $x^2 - (c_i - c_j)x + (c_i - c_j)^{1-q} = 0$ не имеет решения в Z_{q+1} ни при каких $i \neq j$ и осталось воспользоваться предложением 3.

Предложение 4. *Пусть F_q — конечное поле, $q = q_1^k$. Тогда всякая функция $f: F_q \to F_q$ такая, что:*

1) *$f(a) \neq 0$ при любом $a \in F_q$;*

2) $\left(\dfrac{af(a) - bf(b)}{f(a) - f(b)}\right)^{\frac{q-1}{q_1-1}} \neq 1$ *при любых a, b из F_q определяет конечную проективную плоскость порядка q.*

Доказательство. В предложении 1 в качестве функций $\varphi(x)$, $u(x)$ возьмем функции $\varphi(x) = x^{q_1}$, $u(x) = f(x)$. Тогда множество A_φ есть множество элементов поля F_q вида z^{q_1-1}, $z \in F_q$, $z \neq 0$. Теперь предложение 4 следует из предложения 1.

Неизвестно есть ли поля F, удовлетворяющие хотя бы одному из предложений этой работы. Важную роль при выборе функции φ в доказательстве следствий теоремы 1 сыграла работа [2].

Представляют интерес и другие «деформации» тернара $\langle abc \rangle = ab + c$ для конечного поля F.

1. *Холл М.* Комбинаторика.— М. : Мир, 1970.— 424 с.
2. *Музычук М. Е.* Группы автоморфизмов графа Пэли // Вопросы теории групп и гомологической алгебры.— Ярославль, 1987.— С. 64—68.

Киев. ун-т

Получено 28.01.87